International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 3, Issue 5, Dec 2013, 19-26
© TJPRC Pvt. Ltd.

CLOUD COMPUTING: A DATA SECURITY FRAMEWORK

AMAN KUMAR SHARMA[1], ANITA GANPATI[2] & ANJU BALA[3]

[1,2]Associate Professor, Department of Computer Science, H. P. University, Shimla, Himachal Pradesh, India

[3]Assistant Professor, Department of Computer Science, Shoolini University, Solan, Himachal Pradesh, India

ABSTRACT

Cloud computing offers new approach of computing that provides the significant efficiency and economic benefits. Its importance is increasing day by day and receiving a huge attention in the scientific and industrial fields. Although it has many benefits yet has a significant limitation that is security. This study concerns about the security issues of data. This paper firstly explains various data security issues and then possible solutions. First one is an authentication model that provides more secure access to data on cloud, second one is cryptography that encrypts the data to make it more secure, third one is structural method that break the data structurally to avoid the misuse of data and fourth one is a data insurance method which provides an alternate method that assures the data security to user.

KEYWORDS: Cloud Computing, Security Issues, Two Tier Architecture, Data Insurance

INTRODUCTION

Cloud computing is a deliverable model that uses internet and central remote servers and allows consumers and businesses to use applications without installation and access their files at any computer. It plays an important role to reduce the expenditure on resources as well as to improve organization's performance. The cloud computing has gained widespread acceptance due to its expertise in organising and provisioning computational resources. The growth in field of cloud computing increases threat security aspects. Security is considered one of the most critical aspects in everyday computing, and it is no different for cloud computing due to the sensitivity and importance of data stored in the cloud. Cloud Computing has several major issues and concerns, such as data security, trust, regulations, expectations and performance issues. The aim of this study is to examine the major data security issues affecting cloud systems and the solutions available.

Cloud Computing

Cloud computing technology is a concept of providing dramatically scalable and bandwidth, virtualized resources, hardware and software on demand to consumers. Consumers could typically requests cloud services via a web browser or web service [9].

Cloud computing is a model for enabling convenient and on-demand network access to a shared pool of configurable computing resources (e.g. servers, networks, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [8]. The cloud model is composed of five essential characteristics, four deployment models and three service models.

Characteristics

The key characteristics of cloud computing include on-demand self service, broad network access, resource pooling, rapid elasticity and metered service similar to a utility.

- **On-Demand Self Service:** A consumer can unilaterally provision computing capabilities, such as network storage and server time, as needed automatically without requiring human interaction with each service provider.
- **Broad Network Access:** Cloud capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms such as laptops, mobile phones and PDAs.
- **Resource Pooling:** The provider's computing resources are pooled together to serve multiple consumers using multiple-tenant model, with different virtual and physical resources dynamically assigned and reassigned according to consumer requirement. The resources include among others processing, storage, network bandwidth, memory, email services and virtual machines. The pooling together of the resource builds economies of scale [12].
- **Rapid Elasticity:** Cloud services can be elastically and rapidly provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- **Metered Service:** Cloud computing resource usage can be controlled measured and reported providing transparency for both the provider and consumer of the utilised service. Cloud computing services use a metering facility which enables to control and optimise resource use. This implies that just like electricity, IT services, air time or municipality water are charged per usage metrics – pay per use. The more utilization higher is the bill. Just as utility companies sell power to subscribers, and telephone companies charge for air time and data services, IT services such as data centre hosting, network security management or even departmental billing can now be easily delivered as a contractual service.

Deployment Models

There are two initial forms of cloud computing public cloud and private cloud. A public cloud is considered as a multitenant architecture, the private cloud is considered as a proprietary architecture which provides hosted services to a limited number of people behind a firewall. Hybrid clouds incorporate both public and private clouds within the same network. It allows the organisations to benefit from both deployment models.

Private Cloud

Private cloud emulates the concept of cloud computing on a private network. They allow users to have the advantages of cloud computing without some of the pitfalls. It gives complete control over what security measures are in place and how data is managed. This can lead to users having more confidence and control. The major issue with this deployment model is that the users have large expenditures as they have to buy the infrastructure to run the cloud and also have to manage the cloud themselves [3].

Community Cloud

The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g. security requirements, mission, policy and compliance considerations). It may be managed, operated and owned by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public Cloud

Public cloud is the most common type of cloud. This is cloud where multiple users can access web applications and services over the internet. It may be managed, operated and owned by a academic, government organization or business, or some combination of them. It exists on the premises of the cloud provider.

Hybrid Cloud

Hybrid cloud is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g. cloud bursting for load balancing between clouds) [12].

Service Models

Cloud computing is often divided into three main service types: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) and each impacts data control and governance a little differently. With IaaS, the customer may have full control of the actual server configuration granting them more risk management control over the environment and data. In PaaS, the provider manages the hardware and underlying operating system which limits enterprise risk management capabilities on those components. With SaaS, both the platform and the infrastructure are fully managed by the cloud provider which means if the underlying operating system or service isn't configured properly the data in the higher layer application may be at risk [10].

Software as a Service (Saas)

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications can be accessible from various client devices through either a thin client interface, such as program interface or a web browser. The user cannot manage or control the underlying cloud infrastructure including servers, network, storage, operating systems, or even individual application capabilities, with the possible exception of limited consumer specific application configuration settings [12].

Platform as a Service (Paas)

Platform-as-a-Service (PaaS) is a model of software deployment whereby the computing platform is provided as an on-demand service upon which applications can be developed and deployed. Its main purpose is to reduce the cost and complexity of housing, buying and managing the underlying hardware and software components of the platform, including any needed database and program development tools [11]. The consumer does not manage or control the underlying cloud infrastructure including network, operating systems, servers or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (Iaas)

The capability provided to the consumer is to provision processing, networks, storage and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which may include operating systems and applications. The user does not manage or control the underlying cloud infrastructure but has control over storage, operating systems and deployed applications; and possibly limited control of select networking components [12].

DATA SECURITY ISSUES

Cloud computing has number of issues related to data security. According to data protection law "It should be always clear where personal data is located, by whom it is processed and who is responsible for data processing."

But cloud computing conflicts this statement because cloud project via the internet and it is no longer clear which data protection authorities at which location are responsible for ensuring the observance of the principles of data protection [16]. The architecture of cloud computing has three main entities:

User: Users, who have data to be stored in the cloud and rely on the cloud for data computation, consisting of both individual consumers and organizations.

Cloud Service Provider (CSP): A CSP, who has significant resources and expertise in building and managing distributed cloud storage servers, owns and operates live cloud computing systems.

Third Party Auditor (TPA): An optional TPA, who has expertise and capabilities that users may not have, is trusted to assess and expose risk of cloud storage services on behalf of the users upon request [2].

In cloud computing users are the one who store their data on cloud servers with the help of cloud service provider. After that user interacts with cloud servers through CSP to access and receive their data whereas TPA is a third party user which has capabilities that users don’t have and can access data on the behalf of users. Here, Data integrity and data availability are two extremely important elements in the provision of cloud-computing services. However, one has to keep in mind that there is an inevitable trade-off here: more data security is likely to lead to reduce availability, in other words, too much security kills performance [1].

There are three main issues of importance: transmission of data, data privacy and data security. Network transmission security is the security of data transmission in networks to ensure that the data in this process will not be intercepted, tampered or replaced. Data storage security refers to the security of data on the storage media, which means non-volatile or fast recovery after loss. This security should be taken into account by software engineers in design stage of cloud storage services.

It includes not only data redundancy and dynamic, but also isolation. Data management security means that storage service providers will collect user information as little as possible and should ensure that the data will not be disclosed to any third party without the user's consent. Security threats faced by cloud computing can come from different sources and different ways [7].

Data Loss

Data loss or leakage can have severe impact on business, brand and reputation, employee, partner, and customer moral and trust. Loss of core intellectual property could have competitive and financial implications also. Depending upon the data that is lost or leaked, there might be compliance violation and legal ramifications [5]. The data being saved on the cloud against fees surely is of importance. The data if lost is likely to cause many implications, in terms of financial loss, defame of reputation, loss of business, legal implications etc. Regenerating the data could be a lengthy time consuming process or it could be possible to do so. However, the data can be lost due to malfunction of computer device.

Data Privacy

Cloud service providers should collect only necessary information from user and should ensure that the data will not be disclosed to any third party without the user’s consent. So, that the data privacy can be maintained [7]. Private data may at times be shared with the outside world to harass or create problem for the cloud user. Hackers may be the cause of such problem.

Data Theft

Because of multi-tenancy nature of the cloud it could act as a ‘honey-pot’ for hackers. If hackers could attack the cloud they can access data of all the companies hosted on that cloud. Hence data can be easily modified or used by the hackers [5]. The data if stolen from the cloud can be used for emotional blackmail, financial transactions or publicised. The data may be intentionally distributed to unwanted person or it may be hacked.

Data Integrity

Clouds require protection against intentional subversion or sabotage of the functionality of a cloud. Within a cloud there are stakeholders: a variety of administrators, subscribers and providers. The ability to partition access rights to each of these groups, while keeping malicious attacks at bay, is a key attribute of maintaining cloud integrity. In a cloud setting, any lack of visibility into a cloud's mechanisms makes it more difficult for subscribers to check the integrity of cloud-hosted applications [15]. The CSP may have malicious intention and may not share the data with the user itself. Subsequently, it may share part of data or tamper data to make the data useless. This may be done intentionally or spyware software may perform the action in the background [13]

Data Transfer

Within the enterprise boundaries, data transmission usually does not require encryption, or must have a simple data encryption measure. For data transmission across enterprise boundaries, both data confidentiality and integrity should be ensured in order to prevent data from being tapped and tampered with by unauthorized users. In other words, only data encryption is not enough. Data integrity is also needed to be ensured. Therefore, it should ensure that transport protocols provide both confidentiality and integrity [4].

PROPOSED SOLUTIONS

Security itself can be delivered from within the cloud. To provide security to the data there are number of solutions present.

Data Loss

To avoid data loss backup mechanism exists with all the cloud service providers. Mirroring of storage devices used better transmission media may reduce data loss. However, if still the data is lost, it is proposed to have the data insured. Depending upon the size of data and the duration the insurance may be executed. On data loss the user may be is compensated by giving the insurance claim. Data insurance can be the method that is used to provide security to the data, which means that user, can make data insured by giving authorization to a private organization to provide security to data other than the cloud service providers. In this model, all the care of data is taken by the private organization such as where the data is stored, how the data is transferred, availability of data and backup of data. They provide appropriate security measures that will protect their customer’s data and build up confidence for their services. They also place a check on the cloud service providers so that they also cannot breach the information. This method countermeasure for data loss and provide a level of satisfaction to the user that his data is in safe hands.

Data Privacy

As hackers might intrude to access data. It is proposed to have two-tier architecture of data security. Identity and access management is a critical function for every organization, and a fundamental expectation of customers is that the “principle of least privilege” is granted to their data. The principle of least privilege states that only the minimum access necessary to perform an operation should be granted, and that access should be granted only for the minimum amount of time necessary. And this access can only be granted after proper authentication. Here, a new authentication model is proposed that uses two-tier architecture.

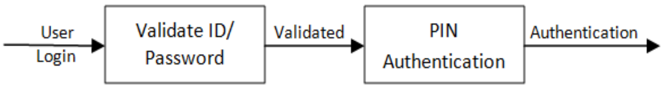

Figure 1: Two Tier Architecture

In this two tier architecture, an alternate authentication PIN is provided. After the successful login in the system user is provided with another authentication PIN. And only after the entry of that PIN user is authorized to access the data. The PIN can be provided to user through two different mediums:

- **E-mail:** The secure code can only be sent to the registered e-mail id of the user. This e-mail id is registered when the data is stored on the cloud or when user is registered on the cloud. It cannot be changed when the user is trying to access data.
- **Mobile Phone/ Landline:** the secure code can also be provided to user through SMS or call. The call can be system generated or cloud service provider can hire some people to do these kinds of calls.

Data Theft

It should be attempted to avoid the data steal. This can be again accomplished by the use of two-tier architecture as discussed earlier. Also besides that encryption of data may be performed. Cryptography could help increasing adoption of Cloud Computing by skeptic or more security concerned companies. Cryptography is the most employed practice to sensitive data [14], thoroughly required by industry, state and federal regulations [17]. The level of security where cryptography can help cloud computing is secure storage. The multi-tenant nature of the cloud amplifies these requirements and creates unique challenges with the accessibility and protection of encryption credentials used to ensure data protection [14]. The major handicap of secure storage is that we cannot outsource the processing of this data without decrypting it before or without revealing the keys used for encryption.

Data Integrity

To solve issues pertaining to data integrity, the data record may be structurally broken into parts. Different parts of data may be saved on another CSP or may be on a number of CSPs. By doing so, the CSP may not realize the importance of data. Further, if the data is encrypted it safeguards even better. In case a specific CSP does not adhere to the user request of data, the user may construct data by gathering data from other CSPs.

DATA SECURITY FRAMEWORK

This study proposes a framework that may be used to provide security to data in cloud computing. In this framework all the four solutions given above are combined together to provide a more secure cloud computing. This framework contains four parts that are data encryption, structurally broken data, data insurance and two tier architecture. These all can work together to provide a secure cloud computing. This framework illustrates the working of all solutions together. Firstly the data is stored in the cloud by user is encrypted so, it cannot be easily read out by anyone, then the data is structurally broken that ensures the ‘principle of least privilege’ that means each piece of data is sent to different service providers so that they do not complete data and due to this they cannot misuse data. Each user has a data insured with service provider so that if the data is lost anyway then it is compensated firm by the insurance and for accessing the data user must have to login with a validated ID and password then after successful login he is provided with PIN, upon entering only correct PIN the user is able to access the data. This framework works to ensure the data security to cloud computing.

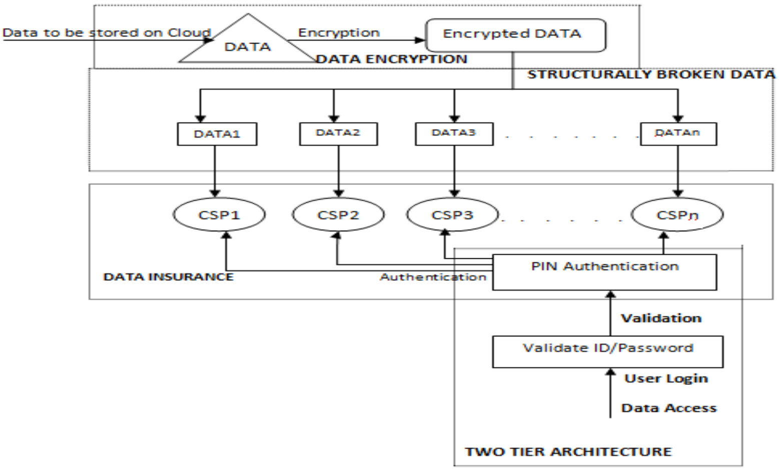

Figure 2: Data Security Framework

CONCLUSIONS

Cloud computing is a distributed architecture that centralizes server resources on a scalable platform so as to provide on demand computing resources and services. Data security is one of the major security concerns in cloud computing as data is the most important thing that is shared in cloud computing environment. In this paper, some of data security issues are discussed. And four solutions are proposed that are Two-tier authorization architecture, cryptography, structural method and data insurance for users which are used to provide security to data.

REFERENCES

1. D. P. Balboni (2011),”Data Protection and Data Security Issues Related to Cloud Computing in the EU,” In Information Security Solutions Europe 2010 Securing Electronic Business Processes, pp. 163-172.

2. P. Bhisikar & A. Sahu (2013),”Security in Data Storage and Transmission in Cloud Computing,” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 3.

3. K. Curran, S. Carlin & M. Adams (2011), “Security issues in cloud computing,” Elixir, 38, 4069-72.

4. D. Chen & H. Zhao (2012): “Data security and privacy protection issues in cloud computing” Paper presented at International Conference In Computer Science and Electronics Engineering (IEEE), 2012 Vol. 1, pp. 647-651.

5. Data Protection Challenges in Cloud Computing an Indian perspective a study report WIPRO 2010, Accessed on August01,2013:http://www.cloudconnectevent.in/presentation/data%20protection%20challenges%20in%20cloud%20computing.pdf

6. P. Dorion (2010): Data destruction services: When data deletion is not enough, viewed on July 6, 2013: http://searchdatabackup.techtarget.com/tip/Data-destruction-services-When-data-deletion-is-not-enough

7. Du Meng (2013): "Data security in cloud computing," Paper presented at Computer Science & Education (ICCSE), 2013 8th International Conference, pp.810,813, 26-28 April 2013

8. Gartner (2011): Gartner identifies the Top 10 strategic technologies for 2011, Accessed on July 01, 2013: http://www.gartner.com/it/page.jsp?id=1454221.

9. G.R. Vijay & A. Rama Mohan Reddy (2013),"Security Issue Analysis in Cloud Computing Environment," International Journal of Engineering Research and Applications, Vol. 3, Issue 1, pp.854-857

10. How Data-Centric Protection Increases Security in Cloud Computing and Virtualization, Accessed on August 15, 2013. https://cloudsecurityalliance.org/wp-content/uploads/2011/11/DataCentricProtection_intheCloud.pdf

11. V. Kumar, M. Swetha, M. S. Muneshwara & S. Prakash (2012),"Cloud Computing: Towards case study of data security mechanism," International Journal of Advanced Technology & Engineering Research, Vol. 2, Issue 4.

12. P. Mell & T. Grance (2009): The NIST Definition of Cloud Computing. Technical Report 15, National Institute of Standards and Technology, www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf

13. R. Mogull (2009): Cloud Data Security: Archive and Delete (Rough Cut), Accessed on July 26, 2013 https://securosis.com/blog/cloud-data-security-archive-and-delete-rough-cut

14. L. Musthaler (2009):Cost-effective data encryption in the cloud, Network World, Accessed on July 01, 2013 http://www.networkworld.com/newsletters/2009/121409bestpractices.html

15. J. A. Mukundrao & G.P. Vikram (2011), "Enhancing Security in Cloud Computing," In Information and Knowledge Management Vol. 1, No. 1, pp. 40-44.

16. Accessed on August 20, 2013. http://whoswholegal.com/news/features /article/ 18246/

17. L.Yan, C. Rong & G. Zhao (2009),"Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography," Cloud Computing pp. 167-177.Springer Berlin Heidelberg.